UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/822,068	04/09/2004	Jung-Soo Jung	678-1443	2064

66547 7590 07/16/2008
THE FARRELL LAW FIRM, P.C.
333 EARLE OVINGTON BOULEVARD
SUITE 701
UNIONDALE, NY 11553

EXAMINER	
LOUIE, OSCAR A	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
07/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.**	**Applicant(s)**	
	10/822,068	JUNG ET AL.	
	Examiner	**Art Unit**	
	OSCAR A. LOUIE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _06 May 2008_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-7,9-14 and 16-36_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-7,9-14 and 16-36_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. In view of the appeal brief filed on 05/06/2008, PROSECUTION IS HEREBY REOPENED. New grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Claim Objections

2. Claims 1, 9, 13, 14, 17, 19, 20, 22, 24, 25, 31, 34, 36 are objected to because of the following informalities:

- Claim 1 line 1 recites the term "for" which should be "…configured to…";
- Claim 1 line 4 recites the term "for" which should be "…of…";

- Claim 1 line 10 recites the term "when" which should be "…if…";
- Claim 9 line 1 recites the term "for" which should be "…configured to…";
- Claims 9 line 3 recites the term "for" which should be "...of...";
- Claim 9 line 10 recites the term "when" which should be "…if…";
- Claim 10 line 2 recites the term "when" which should be "…if…";
- Claim 11 line 3 recites the term "when" which should be "…if…";
- Claim 17 line 1 recites the term "for" which should be "…configured to…";
- Claim 17 line 4 recites the term "for" which should be "…of…";
- Claim 19 line 1 recites the term "for" which should be "…configured to…";
- Claim 19 line 4 recites the term "for" which should be "…of…";
- Claim 19 line 10 recites the term "when" which should be "…if…";
- Claim 20 line 1 recites the term "for" which should be "…configured to…";
- Claim 20 line 4 recites the term "for" which should be "…of…";
- Claim 20 line 11 recites the term "when" which should be "…if…";
- Claim 22 line 1 recites the term "for" which should be "…configured to…";
- Claim 22 line 3 recites the term "for" which should be "…of…";
- Claim 24 line 1 recites the term "for" which should be "…configured to…";
- Claim 24 line 3 recites the term "for" which should be "…of…";
- Claim 25 line 2 recites the term "for" which should be "…configured to…";
- Claim 25 line 3 recites the term "for" which should be "…of…";
- Claim 25 line 19 recites the term "when" which should be "…if…";
- Claim 31 lines 2, 3, 7, & 12 recite the term "for" which should be "…configure to…";

- Claim 31 line 17 recites the term “when” which should be “…if…”;
- Claim 34 line 2 recites the term “when” which should be “…if…”;
- Claim 36 line 7 recites the term “when” which should be “…if…”;

Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 5-7, 9, 13, 14, 16, 20-27, 31, 34, & 36 are rejected under 35 U.S.C. 102(e) as being anticipated by Pirila (US-6674860-B1).

Claim 1:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station “base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations” [column 6 lines 29-34], a method for receiving the broadcast service in a mobile station comprising,

- "generating a registration message including a predetermined registration identifier for identification of the encryption information" (i.e. "A key number 71 is used for determining the current decryption key. A mobile station starts using a new decryption key at the moment when the key number changes") [column 7 lines 39-42];
- "transmitting the generated registration message to a base station" (i.e. "In step 81 the mobile station MS starts the location update procedure") [column 7 lines 60-62];
- "receiving updated encryption information for decryption of the broadcast data from the base station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station" (i.e. "If the user of the mobile station has the right to use the mobile station based location service, the acknowledge contains the current decryption key for the broadcast location information and possibly a decryption key for the next period") [column 8 lines 7-11];
- "updating the registration identifier based on the updated encryption information" (i.e. "If the user of the mobile station has the right to use the mobile station based location service, the acknowledge contains the current decryption key for the broadcast location information and possibly a decryption key for the next period") [column 8 lines 7-11].

Claim 5:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for receiving the broadcast service in a mobile station, as in Claim 1 above, further comprising,

- "the registration message is a message that is transmitted from the mobile station to the base station for a predetermined time while the mobile station is using a broadcast service" (i.e. "In step 81 the mobile station MS starts the location update procedure") [column 7 lines 60-62].

Claim 6:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for receiving the broadcast service in a mobile station, as in Claim 1 above, further comprising,

- "the encryption information is generated by a packet data service node and transmitted to the mobile station via the base station" (i.e. "The mobile station can receive the decryption key from a base station in response to a request or in connection with location update") [column 6 lines 64-66].

Claim 7:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for receiving the broadcast service in a mobile station, as in Claim 1 above, further comprising,

- "the encryption information is generated by the base station and transmitted to the mobile station" (i.e. "The mobile station can receive the decryption key from a base station in response to a request or in connection with location update") [column 6 lines 64-66].

Claim 9:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for providing by a base station the broadcast service to a mobile station comprising,

- "receiving a registration message including a registration identifier transmitted from the mobile station" (i.e. "The mobile station can receive the decryption key from a base station in response to a request or in connection with location update") [column 6 lines 64-66];
- "determining whether the received registration identifier for identification of encryption information required for decryption of the broadcast data is different from a currently valid registration identifier" (i.e. "In step 82 the new mobile switching center MSC/visitor location register VLR requests from the mobile station the information concerning the previous visitor location register and informs the home location register HLR that the visitor location register has been changed, step 83") [column 7 lines 62-66];
- "transmitting an updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from the registration identifier currently valid in the base station" (i.e. "If the user of the mobile station has the right to use the mobile station based location service, the acknowledge contains the current decryption key for the broadcast location information and possibly a decryption key for the next period") [column 8 lines 7-11].

Claim 13:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for providing by a base station the broadcast service to a mobile station, as in Claim 9 above, further comprising,

- "performing an accounting process on the mobile station through a packet data service node when the base station transmits updated encryption information to the mobile station" (i.e. "The invention facilitates real-time, continuous location calculation in speech, data and standby modes because the location of the mobile station is calculated in the mobile station. Since the location information is encrypted, it is possible to make the location service available to only those who specifically order the service, and the use of the service is chargeable. Charging may be based on the delivery of decryption keys or it may be in the form of monthly billing, for example") [column 4 lines 16-21].

Claim 14:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for providing by a base station the broadcast service to a mobile station, as in Claim 9 above, further comprising,

- "holding a current state of the mobile station for a predetermined lifetime of the encryption information when the registration identifier of the mobile station is identical to a registration identifier available in the base station" (i.e. "In addition, a validity period may be given for the decryption key") [column 7 lines 8-9].

Claim 16:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for providing by a base station the broadcast service to a mobile station, as in Claim 9 above, further comprising,

- "transmitting a predetermined response message to the mobile station in response to the registration message if it is determined that transmission of the updated encryption information is not necessary" (i.e. "The mobile station sends to a mobile switching center a [Periodic Location Update Request] and the system returns a [Location Update Acknowledge]") [column 7 lines 1-4].

Claim 20:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for receiving the broadcast service in the mobile station comprising,

- "generating a registration message for use of the broadcast service" (i.e. "Transfer to the base station can be realized e.g. in response to a request sent by the system to the mobile station") [column 6 lines 46-47];
- "transmitting the generated registration message to the base station within a predetermined skew time before a lifetime of current encryption information expires" (i.e. "In addition, a validity period may be given for the decryption key… If a mobile station has been shut down and is turned on, it is possible to transfer in the first location update both the current decryption key and the next decryption key provided that the next change of decryption keys occurs before the next location update, cf. mobile station MS3 in FIG. 5") [column 7 lines 8-9 & 18-23];
- "receiving current encryption information and next encryption information including their lifetimes from the base station in response to the registration message" (i.e. "In addition, a validity period may be given for the decryption key… If a mobile station has been shut down and is turned on, it is possible to transfer in the first location update both the current decryption key and the next decryption key provided that the next change of decryption keys occurs before the next location update, cf. mobile station MS3 in FIG. 5") [column 7 lines 8-9 & 18-23];
- "continuously decrypting the broadcast data using the next encryption information when the lifetime of the current encryption information expires" (i.e. "it is possible to transfer in the first location update both the current decryption key and the next decryption key provided that the next change of decryption keys occurs before the next location update, cf. mobile station MS3 in FIG. 5") [column 7 lines 19-23].

Claim 21:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for receiving the broadcast service in the mobile station, as in Claim 20 above, further comprising,

- "the predetermined skew time is set to a time longer than a maximum period among registration message transmission periods of all mobile stations receiving a broadcast service in a service area of the base station" (i.e. "it is preferable to carry out the change of decryption keys in periods of time that are longer than the location update period") [column 7 lines 14-16].

Claim 22:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for providing by a base station the broadcast service to a mobile station comprising,

- "receiving a registration message for use of the broadcast service by the mobile station" (i.e. "The mobile station can receive the decryption key from a base station in response to a request or in connection with location update") [column 6 lines 64-66];
- "transmitting current encryption information and next encryption information including their lifetimes to the mobile station if it is determined that the registration message was received within a predetermined skew time before the lifetime of the current encryption information expires" (i.e. "In addition, a validity period may be given for the decryption key… If a mobile station has been shut down and is turned on, it is possible to transfer in the first location update both the current decryption key and the next decryption key provided that the next change of decryption keys occurs before the next location update, cf. mobile station MS3 in FIG. 5") [column 7 lines 8-9 & 18-23].

Claim 23:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for providing by a base station the broadcast service to a mobile station, as in Claim 22 above, further comprising,

- "the skew time is set to a time longer than a maximum period among registration message transmission periods of all mobile stations receiving broadcast service in a service area of the base station" (i.e. "it is preferable to carry out the change of decryption keys in periods of time that are longer than the location update period") [column 7 lines 14-16].

Claim 24:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for providing by a base station the broadcast service to a mobile station comprising,

- "receiving a predetermined registration message for use of the broadcast service by the mobile station" (i.e. "The mobile station can receive the decryption key from a base station in response to a request or in connection with location update") [column 6 lines 64-66];
- "transmitting next encryption information following current encryption information to the mobile station if it is determined that the registration message was received within a predetermined skew time before a lifetime of the current encryption information expires" (i.e. "In addition, a validity period may be given for the decryption key… If a mobile station has been shut down and is turned on, it is possible to transfer in the first location

update both the current decryption key and the next decryption key provided that the next change of decryption keys occurs before the next location update, cf. mobile station MS3 in FIG. 5") [column 7 lines 8-9 & 18-23].

Claim 25:

Pirila discloses in a wireless communication system including a base station for providing a broadcast service to at least one mobile station over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to the mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34] comprising,

- "transmitting, by the mobile station, a first registration message for initial use of the broadcast service to the base station" (i.e. "Transfer to the base station can be realized e.g. in response to a request sent by the system to the mobile station") [column 6 lines 46-47];
- "upon receiving the first registration message, transmitting by the base station encryption information for decryption of the broadcast data to the mobile station" (i.e. "The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations.") [column 6 lines 30-34];

- "upon receiving the encryption information, generating by the mobile station a registration identifier which includes identification information of the encryption information" (i.e. "A key number 71 is used for determining the current decryption key. A mobile station starts using a new decryption key at the moment when the key number changes") [column 7 lines 39-42];
- "generating by the mobile station a second registration message including the registration identifier" (i.e. "In step 81 the mobile station MS starts the location update procedure") [column 7 lines 60-62];
- "transmitting the generated second registration message to the base station if second or later registration for use of the broadcast service by the mobile station is required" (i.e. "In step 81 the mobile station MS starts the location update procedure") [column 7 lines 60-62];
- "comparing by the base station the registration identifier included in the second registration message with a registration identifier of encryption information currently registered in the base station" (i.e. "In step 82 the new mobile switching center MSC/visitor location register VLR requests from the mobile station the information concerning the previous visitor location register and informs the home location register HLR that the visitor location register has been changed, step 83") [column 7 lines 62-66];
- "transmitting updated encryption information to the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently registered in the base station" (i.e. "If the user of the mobile station has the right

to use the mobile station based location service, the acknowledge contains the current decryption key for the broadcast location information and possibly a decryption key for the next period") [column 8 lines 7-11].

Claim 26:

Pirila discloses in a wireless communication system including a base station for providing a broadcast service to at least one mobile station over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to the mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], as in Claim 25 above, further comprising,

- "requesting by the base station an accounting process on the mobile station through the packet data service node if the registration identifiers are different" (i.e. "The invention facilitates real-time, continuous location calculation in speech, data and standby modes because the location of the mobile station is calculated in the mobile station. Since the location information is encrypted, it is possible to make the location service available to only those who specifically order the service, and the use of the service is chargeable. Charging may be based on the delivery of decryption keys or it may be in the form of monthly billing, for example") [column 4 lines 16-21].

Claim 27:

Pirila discloses in a wireless communication system including a base station for providing a broadcast service to at least one mobile station over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to the mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], as in Claim 25 above, further comprising,

- "holding by the base station the current encryption information of the mobile station" (i.e. "In addition, a validity period may be given for the decryption key") [column 7 lines 8-9];
- "deferring an accounting process on the mobile station if the registration identifiers are identical" (i.e. "The invention facilitates real-time, continuous location calculation in speech, data and standby modes because the location of the mobile station is calculated in the mobile station. Since the location information is encrypted, it is possible to make the location service available to only those who specifically order the service, and the use of the service is chargeable. Charging may be based on the delivery of decryption keys or it may be in the form of monthly billing, for example") [column 4 lines 16-21].

Claim 31:

Pirila discloses a wireless communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34] comprising,

- "at least one mobile station connected to the base station through the radio channel, for performing location registration for use of the broadcast service" (i.e. "Transfer to the base station can be realized e.g. in response to a request sent by the system to the mobile station") [column 6 lines 46-47];
- "decrypting the broadcast data using the predetermined encryption information transmitted via the base station while using the broadcast service" (i.e. "The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations.") [column 6 lines 30-34];
- "generating a registration identifier as identification information of the encryption information" (i.e. "A key number 71 is used for determining the current decryption key. A mobile station starts using a new decryption key at the moment when the key number changes") [column 7 lines 39-42];

- "transmitting the generated registration identifier to the base station" (i.e. "In step 81 the mobile station MS starts the location update procedure") [column 7 lines 60-62];
- "at least one base station for transmitting to the mobile station broadcast data transmitted via the packet data service node while the mobile station is using the broadcast service" (i.e. "In step 81 the mobile station MS starts the location update procedure") [column 7 lines 60-62];
- "receiving a predetermined registration message transmitted during location registration of the mobile station" (i.e. "In step 81 the mobile station MS starts the location update procedure") [column 7 lines 60-62];
- "analyzing a registration identifier of the encryption information included in the predetermined registration message" (i.e. "In step 82 the new mobile switching center MSC/visitor location register VLR requests from the mobile station the information concerning the previous visitor location register and informs the home location register HLR that the visitor location register has been changed, step 83") [column 7 lines 62-66];
- "determining whether to update the encryption information for the mobile station when the registration identifier transmitted by the mobile station is different from a registration identifier currently valid in the base station" (i.e. "If the user of the mobile station has the right to use the mobile station based location service, the acknowledge contains the current decryption key for the broadcast location information and possibly a decryption key for the next period") [column 8 lines 7-11].

Claim 34:

Pirila discloses a wireless communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], as in Claim 31 above, further comprising,

- "the base station performs an accounting process on the mobile station through the packet data service node when the base station transmitted updated encryption information to the mobile station" (i.e. "The invention facilitates real-time, continuous location calculation in speech, data and standby modes because the location of the mobile station is calculated in the mobile station. Since the location information is encrypted, it is possible to make the location service available to only those who specifically order the service, and the use of the service is chargeable. Charging may be based on the delivery of decryption keys or it may be in the form of monthly billing, for example") [column 4 lines 16-21].

Claim 36:

<u>Pirila</u> discloses a wireless communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], as in Claim 31 above, further comprising,

- "the encryption information can be used for decryption of the broadcast data only for a predetermined lifetime" (i.e. "In addition, a validity period may be given for the decryption key") [column 7 lines 8-9];
- "wherein the base station transmits to the mobile station both current encryption information and next encryption information including their lifetimes if it is determined that a registration message of the mobile station was received within a predetermined skew time before a lifetime of current encryption information expires" (i.e. "In addition, a validity period may be given for the decryption key… If a mobile station has been shut down and is turned on, it is possible to transfer in the first location update both the current decryption key and the next decryption key provided that the next change of decryption keys occurs before the next location update, cf. mobile station MS3 in FIG. 5") [column 7 lines 8-9 & 18-23];

- "wherein the mobile station decrypts the broadcast data using the next encryption information when the lifetime of the current encryption information expires" (i.e. "it is possible to transfer in the first location update both the current decryption key and the next decryption key provided that the next change of decryption keys occurs before the next location update, cf. mobile station MS3 in FIG. 5") [column 7 lines 19-23].

5. Claims 17-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Reeds, III et al. (US-5153919-A).

Claim 17:

Reeds, III et al. disclose in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to the mobile station, "In a mobile cellular telephone arrangement there are many mobile telephones, a much smaller number of cellular radio providers (with each provider having one or more base stations) and one or more switching network providers (common carriers)...To enhance security at other times, three different additional security measures can be employed. They are speech encryption, occasional re-authentication, and control message encryption" [column 4 lines 8-12 & column 9 lines 30-33], a method for receiving a broadcast service in a mobile station comprising,

- "generating a registration message including a predetermined mask key request bit for requesting transmission of the predetermined mask key for decryption of broadcast data" (i.e. "a special random sequence (RANDSSD), and a directive to create a "shared secret data" (SSD) field") [column 4 lines 53-54];

- "transmitting the generated registration message to a base station while the mobile station is using a broadcast service" (i.e. "The CGSA sends the RANDSSD, and the SSD field generation directive, through the base station") [column 4 lines 55-56];
- "receiving the encryption information including the predetermined mask key and lifetime information of the predetermined mask key from the base station based on the mask key request bit" (i.e. "if there is reason to believe that the SSD field has been compromised. At such a time, the home CGSA processor sends another RANDSSD sequence to the mobile unit, and a directive to create a new SSD field") [column 7 lines 4-8].

Claim 18:

Reeds, III et al. disclose in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to the mobile station, "In a mobile cellular telephone arrangement there are many mobile telephones, a much smaller number of cellular radio providers (with each provider having one or more base stations) and one or more switching network providers (common carriers)...To enhance security at other times, three different additional security measures can be employed. They are speech encryption, occasional re-authentication, and control message encryption" [column 4 lines 8-12 & column 9 lines 30-33], a method for receiving a broadcast service in a mobile station, as in Claim 17 above, further comprising,

- "generating another registration message for requesting a new mask key" (i.e. " Having initialized the mobile station, the SSD field remains in force until the home CGSA processor directs the creation of a new SSD field") [column 7 lines 1-3];

- "transmitting the generated registration message to the base station if the lifetime of the mask key has expired" (i.e. "if there is reason to believe that the SSD field has been compromised. At such a time, the home CGSA processor sends another RANDSSD sequence to the mobile unit, and a directive to create a new SSD field") [column 7 lines 4-8].

Claim 19:

Reeds, III et al. disclose in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel "In a mobile cellular telephone arrangement there are many mobile telephones, a much smaller number of cellular radio providers (with each provider having one or more base stations) and one or more switching network providers (common carriers)...To enhance security at other times, three different additional security measures can be employed. They are speech encryption, occasional re-authentication, and control message encryption" [column 4 lines 8-12 & column 9 lines 30-33], a method for providing by a base station the broadcast service to a mobile station comprising,

- "receiving a registration message including a predetermined mask key request bit for requesting transmission of the predetermined mask key for decryption of broadcast data, from the mobile station" (i.e. "The CGSA sends the RANDSSD, and the SSD field generation directive, through the base station") [column 4 lines 55-56];
- "analyzing a value of the predetermined mask key request bit to determine whether to transmit the encryption information including the predetermined mask key and lifetime information of the predetermined mask key" (i.e. "As described in greater detail

hereinafter, in the course of establishing and maintaining a call on a mobile telephony system of this invention, an authentication process may be carried out a number of times throughout the conversation") [column 5 lines 8-12];

- "transmitting the encryption information to the mobile station when the base station determines to transmit the encryption information" (i.e. "if there is reason to believe that the SSD field has been compromised. At such a time, the home CGSA processor sends another RANDSSD sequence to the mobile unit, and a directive to create a new SSD field") [column 7 lines 4-8].

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 2-4, 10-12, 28-30, 32, 33, & 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pirila (US-6674860-B1) in view of Reeds, III et al. (US-5153919-A).

Claim 2:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for receiving the broadcast service in a mobile station, as in Claim 1 above, but Pirila does not explicitly disclose,

- "at least one of a predetermined mask key required for decryption of the broadcast data," although Reeds, III et al. do suggest a shared secret data field, as recited below;
- "generation information for the mask key," although Reeds, III et al. do suggest generation of a new SSD field, as recited below;
- "a lifetime of the mask key," although Reeds, III et al. do suggest an SSD field being compromised requiring the creation of a new SSD field, as recited below;

however, Reeds, III et al. do disclose,

- "a special random sequence (RANDSSD), and a directive to create a "shared secret data" (SSD) field" [column 4 lines 53-54];
- "if there is reason to believe that the SSD field has been compromised. At such a time, the home CGSA processor sends another RANDSSD sequence to the mobile unit, and a directive to create a new SSD field" [column 7 lines 4-8];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "at least one of a predetermined mask key required for decryption of the broadcast data" and "generation information for the mask key" and "a lifetime of the mask key," in the invention as disclosed by Pirila for the purposes of providing improved security of communications by having an additional controlled secret key that, "only the base stations which successfully interacted with the mobile unit have the shared secret data field; and that number can be limited by the provider simply by directing the mobile unit to create a new shared secret data field" [column 3 lines 27-32].

Claim 3:

Pirila and Reeds, III et al. disclose in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for receiving the broadcast service in a mobile station, as in Claim 2 above, but Pirila does not explicitly disclose,

- "the registration identifier includes a hash value determined by applying a hash function to a corresponding predetermined mask key each time the mask key is updated," although Reeds, III et al. do suggest hashing, as recited below;

however, Reeds, III et al. do disclose,

- "Many authentication processes use a hashing function, or a one-way function, to implement the processes" [column 5 lines 17-18];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the registration identifier includes a hash value determined by applying a hash function to a corresponding predetermined mask key each time the mask key is updated," in the invention as disclosed by Pirila for the purposes of providing authentication.

Claim 4:

Pirila and Reeds, III et al. disclose in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for receiving the broadcast service in a mobile station, as in Claim 2 above, but Pirila does not explicitly disclose,

- "the registration identifier includes a sequence number sequentially assigned to a corresponding predetermined mask key each time the mask key is updated," although Reeds, III et al. do suggest a sequence part of an authentication string, as recited below;

however, Reeds, III et al. do disclose,

- "...the RANDSSD sequence to form an authentication string" [column 6 line 9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the registration identifier includes a sequence number sequentially assigned to a corresponding predetermined mask key each time the mask key is updated," in the invention as disclosed by Pirila for the purposes of generating a new SSD field associated with an ESN and RANDSSD.

Claim 10:

Pirila discloses in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for providing by a base station the broadcast service to a mobile station, as in Claim 9 above, but Pirila does not explicitly disclose,

- "at least one of a predetermined mask key required for decryption of the broadcast data," although Reeds, III et al. do suggest a shared secret data field, as recited below;
- "generation information for the mask key," although Reeds, III et al. do suggest creating a new SSD field, as recited below;
- "a lifetime of the mask key," although Reeds, III et al. do suggest an SSD field being compromised requiring the creation of a new SSD field, as recited below;

however, Reeds, III et al. do disclose,

- "a special random sequence (RANDSSD), and a directive to create a "shared secret data" (SSD) field" [column 4 lines 53-54];
- "if there is reason to believe that the SSD field has been compromised. At such a time, the home CGSA processor sends another RANDSSD sequence to the mobile unit, and a directive to create a new SSD field" [column 7 lines 4-8];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "at least one of a predetermined mask key required for decryption of the broadcast data" and "generation information for the mask key" and "a lifetime of the mask key," in the invention as disclosed by Pirila for the purposes of providing improved security of communications by having an additional controlled secret key that, "only the base stations which successfully interacted with the mobile unit have the shared secret data field; and that number can be limited by the provider simply by directing the mobile unit to create a new shared secret data field" [column 3 lines 27-32].

Claim 11:

Pirila and Reeds, III et al. disclose in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for receiving the broadcast service in a mobile station, as in Claim 10 above, but Pirila does not explicitly disclose,

- "the registration identifier includes a hash value determined by applying a hash function to a corresponding predetermined mask key each time the mask key is updated," although Reeds, III et al. do suggest hashing, as recited below;

however, Reeds, III et al. do disclose,

- "Many authentication processes use a hashing function, or a one-way function, to implement the processes" [column 5 lines 17-18];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the registration identifier includes a hash value determined by applying a hash function to a corresponding predetermined mask key each time the mask key is updated," in the invention as disclosed by Pirila for the purposes of providing authentication.

Claim 12:

Pirila and Reeds, III et al. disclose in a wireless communication system for providing a broadcast service to at least one mobile station over a radio channel, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], a method for receiving the broadcast service in a mobile station, as in Claim10 above, but Pirila does not explicitly disclose,

- "the registration identifier includes a sequence number sequentially assigned to a corresponding predetermined mask key each time the mask key is updated," although Reeds, III et al. do suggest a sequence part of an authentication string, as recited below;

however, Reeds, III et al. do disclose,

- "...the RANDSSD sequence to form an authentication string" [column 6 line 9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the registration identifier includes a sequence number sequentially assigned to a corresponding predetermined mask key each time the mask key is updated," in the invention as disclosed by Pirila for the purposes of generating a new SSD field associated with an ESN and RANDSSD.

Claim 28:

Pirila discloses in a wireless communication system including a base station for providing a broadcast service to at least one mobile station over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to the mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], as in Claim 25 above, but Pirila does not explicitly disclose,

- "the encryption information includes at least one of a predetermined mask key required for decryption of the broadcast data," although Reeds, III et al. do suggest a shared secret data field, as recited below;
- "generation information for the mask key," although Reeds, III et al. do suggest generation of a new SSD field, as recited below;
- "a lifetime of the mask key," although Reeds, III et al. do suggest an SSD field being compromised requiring the creation of a new SSD field, as recited below;

however, Reeds, III et al. do disclose,

- "a special random sequence (RANDSSD), and a directive to create a "shared secret data" (SSD) field" [column 4 lines 53-54];
- "if there is reason to believe that the SSD field has been compromised. At such a time, the home CGSA processor sends another RANDSSD sequence to the mobile unit, and a directive to create a new SSD field" [column 7 lines 4-8];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the encryption information includes at least one of a predetermined mask key required for decryption of the broadcast data" and "generation information for the mask key" and "a lifetime of the mask key," in the invention as disclosed by Pirila for the purposes of providing improved security of communications by having an additional controlled secret key that, "only the base stations which successfully interacted with the mobile unit have the shared secret data field; and that number can be limited by the provider simply by directing the mobile unit to create a new shared secret data field" [column 3 lines 27-32].

Claim 29:

Pirila discloses in a wireless communication system including a base station for providing a broadcast service to at least one mobile station over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to the mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key

314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], as in Claim 28 above, but Pirila does not explicitly disclose,

- "the registration identifier includes a hash value determined by applying a hash function to a corresponding predetermined mask key each time the mask key is updated," although Reeds, III et al. do suggest hashing, as recited below;

however, Reeds, III et al. do disclose,

- "Many authentication processes use a hashing function, or a one-way function, to implement the processes" [column 5 lines 17-18];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the registration identifier includes a hash value determined by applying a hash function to a corresponding predetermined mask key each time the mask key is updated," in the invention as disclosed by Pirila for the purposes of providing authentication.

Claim 30:

Pirila discloses in a wireless communication system including a base station for providing a broadcast service to at least one mobile station over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to the mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key

314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], as in Claim 28 above, but Pirila does not explicitly disclose,

- "the registration identifier includes a sequence number sequentially assigned to a corresponding predetermined mask key each time the mask key is updated," although Reeds, III et al. do suggest a sequence part of an authentication string, as recited below;

however, Reeds, III et al. do disclose,

- "...the RANDSSD sequence to form an authentication string" [column 6 line 9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the registration identifier includes a sequence number sequentially assigned to a corresponding predetermined mask key each time the mask key is updated," in the invention as disclosed by Pirila for the purposes of generating a new SSD field associated with an ESN and RANDSSD.

Claim 32:

Pirila discloses a wireless communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], as in Claim 31 above, but Pirila does not explicitly disclose,

- "the registration identifier includes a hash value determined by applying a hash function to a corresponding mask key each time the mask key is updated," although Reeds, III et al. do suggest hashing, as recited below;

however, Reeds, III et al. do disclose,

- "Many authentication processes use a hashing function, or a one-way function, to implement the processes" [column 5 lines 17-18];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the registration identifier includes a hash value determined by applying a hash function to a corresponding mask key each time the mask key is updated," in the invention as disclosed by Pirila for the purposes of providing authentication.

Claim 33:

Pirila discloses a wireless communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], as in Claim 31 above, but Pirila does not explicitly disclose,

- "the registration identifier includes a sequence number sequentially assigned to a corresponding mask key each time the mask key is updated," although Reeds, III et al. do suggest a sequence part of an authentication string, as recited below;

however, Reeds, III et al. do disclose,

- "...the RANDSSD sequence to form an authentication string" [column 6 line 9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the registration identifier includes a sequence number sequentially assigned to a corresponding mask key each time the mask key is updated," in the invention as disclosed by Pirila for the purposes of generating a new SSD field associated with an ESN and RANDSSD.

Claim 35:

Pirila and Reeds, III et al. disclose a wireless communication system including a base station for providing a broadcast service to a plurality of mobile stations over a radio channel and a packet data service node for connecting the base station to a content server via a packet data network, wherein broadcast data is sequentially encrypted with different encryption information and provided to a mobile station "base station BTSA is the base station serving the mobile station 31. The serving base station BTSA sends to the mobile station 31 information about the decryption key 314 used in the location process, whereby the mobile station decrypts the location information received from base stations" [column 6 lines 29-34], as in Claim 32 above, but Pirila does not explicitly disclose,

- "the base station receives a registration message including a predetermined mask key request bit for requesting transmission of the mask key from the mobile station while the mobile station is using a broadcast service," although Reeds, III et al. do suggest a base station receiving an SSD field and RANDSSD, as recited below;
- "transmitting predetermined encryption information including the mask key and lifetime information of the mask key to the mobile station if the mask key request bit has a predetermined bit value," although Reeds, III et al. do suggest creating a new SSD field if the SSD field has been compromised, as recited below;

however, Reeds, III et al. do disclose,

- "The CGSA sends the RANDSSD, and the SSD field generation directive, through the base station" [column 4 lines 55-56];
- "if there is reason to believe that the SSD field has been compromised. At such a time, the home CGSA processor sends another RANDSSD sequence to the mobile unit, and a directive to create a new SSD field" [column 7 lines 4-8];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the base station receives a registration message including a predetermined mask key request bit for requesting transmission of the mask key from the mobile station while the mobile station is using a broadcast service" and "transmitting predetermined encryption information including the mask key and lifetime information of the mask key to the mobile station if the mask key request bit has a predetermined bit value," in the invention as disclosed by Pirila for the purposes of providing improved security of communications by having an additional controlled secret key that, "only the base stations which successfully interacted with the mobile unit have the shared secret data field; and that number can be limited by the provider simply by directing the mobile unit to create a new shared secret data field" [column 3 lines 27-32].

Response to Arguments

8. Applicant's arguments, see pages 8-33, filed 05/06/2008, with respect to the rejection(s) of claim(s) 1-7, 9-14, & 16-36 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of newly found prior art references Pirila (US-6674860-B1) and Reeds, III et al. (US-5153919-A).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Alanara et al. (US-5594797-A) – mask value XORing

b. Brown et al. (US-5793866-A) – common secret number mask encrypting A-Key

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
07/12/2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136